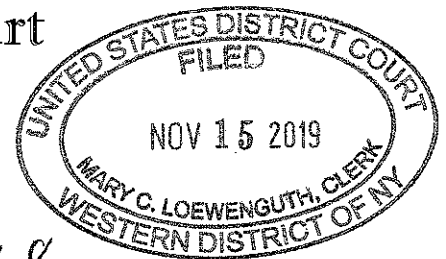


United States District Court
for the
Western District of New York



In the Matter of the Search of

(Briefly describe the property to be searched or identify the person by name and address.)

The Cellular Towers Owned by Cellco Partnership,
DBA Verizon Wireless, that provided cell site location
Information and any other relevant information for
telephone number 845-521-9184

19-MJ- 4168

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property located in the Western District of New York *(identify the person or describe the property to be searched and give its location)*: The Cellular Towers Owned by Cellco Partnership, DBA Verizon Wireless, that provided cell site location information and any other relevant information for telephone number 845-521-9184.

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:

See Attachment A, Schedule of Items to be Seized, which attachment is incorporated by reference as if fully set forth herein, all of which are fruits, evidence and instrumentalities of a violation of Title 18, United States Code, Sections 2252A and 2261A.

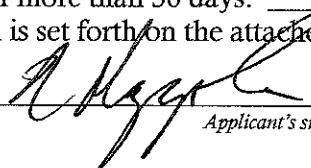
The basis for search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: Title 18, United States Code, Sections 2252A and 2261A.

The application is based on these facts: *See attached affidavit.*

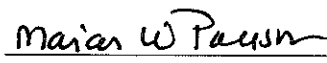
- ☒ continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature

Nicholas Mazzola, TFO FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: November 15, 2019


Judge's signature

City and state: Rochester, New York

Marian W. Payson, U.S. Magistrate Judge
Printed name and Title

ATTACHMENT A

I. The Account

The Search Warrant applies to records and information associated with the cellular telephones assigned call number:

- a. 845-521-9184 ("TARGET CELL TELEPHONE").

II. Records and Other Information to be Disclosed

Cellco Partnership DBA Verizon Wireless is required to disclose the following records and other information, if available, to the United States for the Account listed in Part I of this Attachment.

- A. For a time period of 30 days following the execution of this Search Warrant, provide location-based services (e.g. precision data to include true call data, timing advance data, and per-call measurement data.)

III. Records and Other Information to be Disclosed

All information described above in Section II that constitutes evidence of violations of Title 18 U.S.C. § 2252A(a)(2)(A), distribution of child pornography in interstate or foreign commerce by computer and Title 18 U.S.C. § 2261A(2)(B), cyber stalking.

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE)	
APPLICATION OF THE UNITED)	
STATES OF AMERICA FOR)	FILE NO. <u>19-mj-4168</u>
AUTHORIZATION TO OBTAIN)	
PRECISION AND HISTORICAL)	
LOCATION DATA CONCERNING)	TO BE FILED UNDER SEAL
CELLULAR TELEPHONE NUMBER)	
845-521-9184)	

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Nicholas Mazzola, being duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a police investigator employed by the Rochester Police Department and am currently assigned as a Task Force Officer on the FBI Cyber Squad, Buffalo Division, in Rochester, NY. I have been a police officer since 1994, an investigator since 2003, and was assigned to the Major Crimes Unit from January, 2011 to December, 2018. I have attended numerous courses in criminal investigations, and have had the opportunity to conduct, coordinate and or participate in a number of successful investigations involving burglaries, robberies, weapons possession, assaults, larcenies, cyber and economic crimes, and homicides, and have interviewed hundreds of defendants, victims, witnesses and others who have been involved in such offenses.

2. I have been involved in excess of 100 homicide investigations, both as a lead investigator and assisting other investigators. During these investigations I have had the opportunity to be the affiant on numerous search warrants. These warrants were based on the search for evidence to substantiate the crime of murder to include DNA evidence, clothing, weapons (to include firearms and knives), cellular telephones, computers, and numerous other forms of electronic data collection devices. I have personally been the affiant of warrants for cellular telephones that has led to the recovery of evidence recovered in a search in videos, photos, electronic communications (e.g., text messages, sms, cellular communications, GPS, and email communications), downloads, contacts, notes and internet search history/caches related to the possession, purchase, or sale of weapons and ammunition and/or any other evidence related to the commission of a homicide. I have personally been involved in investigations in which GPS and/or Cell Site location information has proven to establish the location of a suspect, victim and/or witness to a murder at a time relevant to the murder investigation, including information placing a suspect(s) at or near the crime scene at the time of the murder. In addition, I have personally observed text, SMS, and/or MMS messaging by people who have committed a crime such as murder to other individuals before and after the crime in which they make statements implicating themselves and in some cases seeking assistance in avoiding apprehension.

3. I am an investigative or law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7); that is, an officer of the United States who is empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Title 18, United States Code, Section 2516.

4. I submit this Affidavit in support of an Application for a Search Warrant pursuant to Federal Rule of Criminal Procedure 41 and 18 U.S.C. § 2703(c)(1)(A), authorizing law enforcement officers to obtain information described in Attachment A for the following cellular telephone number:

- a. 845-521-9184 (hereinafter, "TARGET CELL TELEPHONE"), which is maintained and controlled by Celco Partnership DBA Verizon Wireless (hereinafter, the "PROVIDER"), located at 180 Washington Valley Rd, Bedminster, NJ 07921. The information to be searched and seized is described in the following paragraphs and in Attachment A to the proposed warrant.

5. For the reasons detailed below, there is probable cause to believe that the TARGET CELL TELEPHONE contains evidence, fruits, and instrumentalities of 18 U.S.C. § 2252A, distribution of child pornography that has been transported in interstate or foreign commerce by computer and 18 U.S.C. § 2261A, cyber stalking (hereinafter, "SUBJECT OFFENSES").

6. This affidavit is based upon my personal knowledge, my review of documents and other evidence, and my conversations with other law enforcement agents and civilian witnesses. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

Probable Cause

7. On February 19, 2019, a female (hereinafter, "Victim") was interviewed by members of the FBI. In sum, Victim said she began dating Charles REGALBUTO, DOB: 01/XX/93, on October 14, 2010. Victim was 15 years of age and REGALBUTO was 17 years old and a senior in high school. REGALBUTO went away to college after graduating high school. While in college, REGALBUTO asked Victim to send naked pictures of herself. REGALBUTO told Victim that he would delete the photos. Victim initially declined but later did so. She sent two naked photos of herself via text message from her cell phone to REGALBUTO's cell phone XXX-XXX-9184. The photos showed Victim's breasts and vagina while masturbating in one photo and the Victim's vagina while masturbating in the other. Neither photo showed the Victim's face. The photos were taken by Victim in or around September 2011. Victim said she was 16 or 17 years old at the time. REGALBUTO had also taken two naked photos of Victim in May 2011 in his bedroom in Congers, NY, which showed Victim's full naked body, including her face and vagina. Copies of the photos reviewed by members of the FBI and confirmed to contain the images described above.

8. Victim said REGALBUTO dropped out of college around November 2011. Victim graduated high school in June 2013 and began college at the Rochester Institute of Technology that fall. While at college, her relationship with REGALBUTO deteriorated and ultimately ended on April 17, 2014. That same day, REGALBUTO began to harass, threaten, and torment Victim. He began sending multiple alarming and threatening texts to Victim from his cell phone XXX-XXX-9184 to include the following:

REGALBUTO: Unblock me

REGALBUTO: Ill fucking kill yoy"[Your Affiant believes REGALBUTO intended to text 'you' based on the character 'Y' is next to the character 'U' on traditional U.S. keyboards]

REGALBUTO: Don't forget who has your nudes slut [text message was followed by REGALBUTO sending five photos of Victim to Victim's phone. Of the five photos, two were of Victim previously mentioned (one naked photo of Victim masturbating showing her vagina and one naked photo of Victim in REGALBUTO's bedroom);

REGALBUTO: Twitter or Instagram? [Your Affiant believes this is a reference to which social media platform REGALBUTO was asking to post the naked pictures.];

Victim: Im 17 in most of those and that's literally illegal

REGALBUTO: I don't give a fuck

REGALBUTO: Ill ruin your life the way you ruined mine.....Good youre 17? Maybe ill try to get kid porn pressed against you. And once it's up is out there forever...Congrats im going to go to jail and be a registered sex offender...Youre so lucky I don't have enough service in this building but I swear once I leave it's done.

Victim and REGALBUTO also spoke on the phone that day, at which time he threatened to kill her.

9. On May 26, 2014, REGALBUTO acknowledged he threatened to post Victim's naked photos. At 11:50 pm, REGALBUTO sent a text message to Victim stating, "I fucked up beyond belief and I don't deserve your forgiveness but I love you and I want to make everything ok I want to show you that that's not me".

10. As a result of REGALBUTO's behavior and actions, Victim petitioned the Rockland County Family Court for an order of protection in 2014, which was granted. The order required REGALBUTO to stay at least 200 feet away from Victim and have no contact with her for a period of one year. The contact, based upon text messages provided by the Victim, continued throughout the period of the order of protection and beyond.

11. REGALBUTO routinely used threats of suicide to keep Victim from ending their communications. He would send Victim countless text messages that would go unanswered. Several examples are as follows:

- 10/23/14 at 2:48 am, "You were the worst thing to ever happen to me. You're a dumb cunt who fucked up my whole life and made me a bad person. Thanks [Victim first name], I hope youre fucking happy"

- 10/23/14 at 02:58 am, "The only thing I wanted to do. Was love you.and make.you happy. Why couldn't you let me donthat"

- 10/25/14 at 4:34 am, "Hey"

- 10/25/14 at 2:37 pm, "I dream about you every night"

- 10/25/14 at 3:15 pm, "This is why I'm gonna kill myself"

12. REGALBUTO referenced blackmailing Victim in text messages, said he deleted her photos, only to later say he still had them, as follows:

- 11/22/14 at 2:58 pm, "If it means anything I've deleted all the pics I have of you"

- 11/22/14 at 2:59 pm, "I'm just trying to show you that I'm not that same guy who's gonna try to guilt you or blackmail you. I don't want your pity or your sympathy. I want you to be happy and I want to show you that I'm not an asshole anymore"

- 02/24/15 at 8:26 pm, "I still have pictures of you"

13. Text messages from 4/17/14 to 11/12/16 were extracted and captured from Victim's phone to include the text messages listed above, as well as other long periods of unanswered texts sent by REGALBUTO and exchanges between Victim and REGABUTO, where he stalked and extorted Victim.

14. In November of 2016, Victim changed her cell number. Around the time of December, 2016, Victim began receiving messages by unknown people on Facebook, who would tell her someone claiming to be her boyfriend was posting naked pictures of her on the Internet.

15. On May 18, 2017, Victim was contacted by "Wew Lad" on Facebook. Wew Lad sent her a message, saying a person named "Greg Macdugal" was sharing naked pictures of her on Reddit, among other sites. Wew Lad provided Victim with screen shots of a conversation on Kik between him and "Greg Macdougall frogger7776". The conversation on Kik also had the naked photos of Victim, previously described.

16. In June of 2017, Victim was contacted by a user Maddiegirlphoto on Instagram. The user was blackmailing Victim by asking her for naked pictures to confirm the ones in Maddiegirlphoto's possession were actually her. The messages became

increasingly aggressive and threatening. Maddiegirlphoto sent the naked pictures taken of Victim in REGALBUTO's bedroom, previously described. The user also electronically distributed the same naked photos to Victim's college classmate at RIT and a friend from home.

17. On September 23, 2017, the New York State Police (NYSP) requested information from kik.com regarding user "frogger7776". Results showed the name listed as Greg Macdougall with an email address of frogger7776@gmail.com. Kik also provided 14 pages of IP addresses from 09/15/17 to 10/09/17 associated with this account. An IP address of 69.127.137.176 was listed about 215 times. The IP address 70.214.115.168 was the last one listed in the records provided (10/09/17 at 1555 UTC).

18. In October 2017, Victim was contacted on Facebook by user Ben Peterson. The user told Victim he got her naked pictures from user frogger7776 on Kik. Victim identified the contact from Ben Peterson as an opportunity to identify the IP address of frogger7776. As such, she researched on the Internet and Grabify IP Logger as an online service to do the same. Your Affiant reviewed the website grabify.link and identified a website designed to track the IP addresses of a user specified link. Victim asked Ben Peterson to contact Greg Macdougall and send him the link <http://short.co/NBMJOF.jpg>. If Macdougall were to click on the link, the device information and IP address would be captured through the Grabify website. Ben Peterson sent the link to Greg Macdougall, who subsequently clicked on the link. Victim reviewed a notification sent by Grabify which revealed the device used was an Apple iPhone, from

IP address 69.127.137.176 in Congers, NY, 10/09/17 at 0734 hours EST. The IP address returned to Optimum Online (Cablevision Systems).

19. On October 11, 2017, Victim sent Investigator Solomone (NYSP) a screenshot she received from “Ben Peterson”. The screenshot was a message on Kik from “Greg Macdougall”, indicating anyone could go to <https://www.pornhub.com/album/19817831> to “find his gf”. Investigator Solomone was able to capture nude photos (previously described) of Victim. The pornhub.com user titled the photos as “[Victim first name] Her BF KIK is Frogger7776”.

20. NYSP requested information from Optimum Online for IP address 69.127.137.176 on 10/09/17 at 0734 EST and 09/20/17 at 0302:38 UTC, the latter being a date and time provided by Kik.com documents. Both IP addresses returned to account number 07873-125323-02, subscriber name Kerri Regalbuto of 26 The Rise, Congers, NY 10920, that being the mother and home address of Charles REGALBUTO.

21. NYSP requested information from Verizon Wireless for IP address 70.214.115.168, specifically from 10/09/17 at 1555:10 UTC. The IP address had been obtained from documents provided by Kik. Results from Verizon Wireless showed the IP address returned to a natting router, which means a number of different devices could be connected at the same time. Within the listed phone numbers using IP 70.214.115.168, #845-521-9184 is captured at least ten times. NYSP requested subscriber information from

Verizon Wireless for #XXX-XXX-9184, which showed the subscriber to be Charles Regalbuto of 26 The Rise, Congers, NY, 10920.

22. On 12/08/17, Charles REGALBUTO was interviewed by the NYSP after he was advised of his Miranda rights and waived same. In sum, REGALBUTO provided his date of birth as 01/23/93 and a home address of 26 The Rise, Congers, NY. REGALBUTO said his ex-girlfriend was [Victim first and last name]. He started a Kik account with a user name, frogger7776 and an email frogger7776@gmail.com. REGALBUTO created the account on his cell phone while he was at home. He posted nude pictures of his ex-girlfriend Victim "a few dozen times" to random people from his Kik account. REGALBUTO also posted nude pictures of her 2-3 times after learning she had reported the activity to the police. REGALBUTO provided a signed, written statement to the New York State Police.

23. Victim, through her own research, has identified the same naked pictures of herself on numerous websites. Based upon my training and experience, your Affiant knows that digital images, particularly naked images, are extremely difficult to remove from the Internet. Once those images have been posted, they can be downloaded and reposted in perpetuity. Your Affiant knows that the distribution of these images on numerous websites, whether done directly by REGALBUTO, are undoubtedly a result of his original postings. Your Affiant also knows, based upon my training and experience, that these photos are likely to remaining on the Internet indefinitely.

24. Based on my training and experience, the above described images meet the federal definition of “child pornography”, as defined in Title 18, United States Code, Section 2256(8).

25. On July 18, 2019, Honorable United States Magistrate Judge Jonathan Feldman signed an arrest warrant for Charles REGALBUTO for charges in violation of Title 18, United States Code, Section 2252A(a)(2)(A), distribution of child pornography that has been transported in interstate or foreign commerce by computer and Title 18, United States Code, Section 2261A(2)(B), cyber stalking.

26. On November 12, 2019, your affiant spoke with Victim, who indicated Charles REGALBUTO would contact Victim periodically via Instagram; the most recent communication was in or about August 2019. In August, 2019, Victim called (from a blocked number) REGALBUTO at his known phone number of 845-XXX-XXXX. REGALBUTO did not answer the call, which then went to voicemail. The voicemail recording indicated the caller had reached “Charlie REGALBUTO” and requested the caller to leave a message. Victim said the voicemail was the voice of Charles REGALBUTO.

27. On November 12, 2019 at about 12:15 pm, your affiant also called REGALBUTO at 845-XXX-XXXX from a blocked number. The call went to voicemail and indicated the caller had reached “Charlie REGALBUTO”.

Summary

28. Your Affiant believes that the combination of location services for a period of 30 days, subscriber information, toll records, historical cell tower data, and precision GPS data may contain evidence, fruits, and instrumentalities of the SUBJECT OFFENSES.

29. Additionally, regarding location-based services, your Affiant believes that monitoring the transmissions from the TARGET CELL TELEPHONE will provide the investigating agents the ability to conduct effective surveillance, to identify the user or users of the TARGET CELL TELEPHONE, as well as establish the physical location of the subject and the TARGET CELL TELEPHONE for the purpose of affecting his arrest for committing the TARGET OFFENSES. Such an order would: (1) operate at any time of the day or night as required; (2) would be expressly limited to transmissions needed to ascertain the physical location of the Target Telephone; and (3) would expressly exclude any voice communications transmitted from the Target Telephone.

30. In my training and experience, I have learned that the Provider is a company that provides cellular telephone access to the general public. I also know that providers of cellular telephone service have technical capabilities that allow them to collect and generate information about the locations of the cellular telephones to which they provide service, including cell-site data, also known as "tower/face information" or "cell tower/sector records." Cell-site data identifies the "cell towers" (i.e., antenna towers

covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the “sector” (i.e., faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data provides an approximate location of the cellular telephone but is typically less precise than other types of location information, such as E-911 Phase II data or Global Positioning Device (“GPS”) data. I also know that the Provider captures GPS data or precision data, and sometimes referred to as per-call measurement data, true call data or advanced timing data. This data and its precise details, typically captured in latitude and longitude coordinates is retained for shorter durations. Depending on the provider, the precision data can be retained for approximately one week to two or three months.

31. Based on my training and experience, in addition to traditional subscriber and toll record data, I know that the Provider can collect cell-site and precision data about the TARGET CELL TELEPHONE. I also know that wireless providers such as Verizon Wireless typically collect and retain cell-site data pertaining to cellular phones to which they provide service in their normal course of business in order to use this information for various business-related purposes.

AUTHORIZATION REQUESTED

32. Based on the foregoing, there is probable cause to believe that the Requested Information will lead to locating the suspect involved in the activities described above.

The FBI is requesting, for the phone number identified as the TARGET CELL TELEPHONE:

- a. Location-based services for a period of 30 days following delivery of the Search Warrant to the PROVIDER (e.g. precision data to include true call data, timing advance data, and per-call measurement data);

33. There is “reasonable cause to believe that providing immediate notification of the execution of the Warrant may have an adverse result.” 18 U.S.C. § 3103a(b)(1). Providing prior notice to the subscriber or user of the TARGET CELL TELEPHONE would seriously jeopardize the ongoing investigation, as such a disclosure would give that person an opportunity to destroy evidence, change patterns of behavior, and potentially act out against the victim.

34. The execution of this Warrant will not result in the seizure of any tangible property or any wire or electronic communication (as defined in 18 U.S.C. § 2510). To the extent that the Warrant authorizes the seizure of any stored wire or electronic information, that seizure is expressly authorized by 18 U.S.C. § 2703(c)(1)(A).

35. The government is seeking this information pursuant to Title 18 U.S.C. § 2703(c)(1)(A) and Rule 41. The Service Provider is a provider of an electronic communications service, as defined in 18 U.S.C. § 2510(15). Accordingly, the United States may seek a court order issued under 18 U.S.C. § 2703(c)(1)(A) to require the Service Provider to disclose precise location information pertaining to the Target Cell Telephone.

Further, this Court is a court of competent jurisdiction because it has jurisdiction over the offense being investigated. 18 U.S.C. Section 2711(3).

36. Pursuant to Federal Rule of Criminal Procedure 41 and 18 U.S.C. § 2703(c)(1)(A), it is requested that the Court issue a Warrant and Order authorizing law enforcement officers of the FBI to obtain the Requested Information.


37. It is further requested that the Application, Order, Warrant, and this Affidavit, as it reveals an ongoing investigation, be sealed until further order of the Court in order to avoid premature disclosure of the investigation, guard against flight, and better ensure the safety of law enforcement officers and others, except that working copies may be served on Special Agents and other investigative and law enforcement officers of the FBI, federally deputized state and local law enforcement officers, and other government and contract personnel acting under the supervision of such investigative or law enforcement officers, and the Service Provider as necessary to effectuate the Court's Order.

38. It is further requested that the Service Provider, its affiliates, officers, employees, and agents not disclose the existence of Court's Order, or the existence of the investigation, to the listed subscriber or to any other person, unless and until authorized to do so by the Court.

39. It is further requested that, pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), the Court authorize notice to be delayed for a period

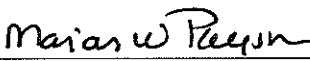
of 6 months after the authorization of this Warrant. Based upon my training and experience, 6 months is a reasonable amount of time to conduct investigations of similar characteristics. The subjects is similar investigations often take extreme measures to avoid attribution and continue the scheme.

40. Your Affiant, therefore, respectfully requests that the attached Warrant be issued authorizing Special Agents of the FBI to ascertain the information described in Attachment A for the TARGET CELL TELEPHONE.



NICHOLAS MAZZOLA
Task Force Officer
Federal Bureau of Investigation

Subscribed and sworn to before me
this 15 day of November, 2019.



MARIAN W. PAYSON
United States Magistrate Judge